Opening Statement of the Honorable Fred Upton
Subcommittee on Energy hearing
"Keeping the Lights On: Addressing Cyber Threats to the Grid"
July 12, 2019

As Prepared for Delivery

Today's hearing continues the Subcommittee's ongoing oversight of cybersecurity threats to the electric grid. While this is the first hearing specifically on that topic this year, the Subcommittee has been raising questions about persistent and emerging threats to the electrical grid in closed briefings and in hearings with federal officials and others over the course of this session—building on the work we've done over the past few Congresses.

It is unquestionable that ensuring the reliable supply of electricity is vital to our nation's security, economy, our health and welfare. Electricity enables telecommunications, financial transactions, the transport and delivery of energy, and agriculture. It powers the infrastructure that delivers our drinking water. It enables business and industry to make and provide the goods and services of our modern society. It powers our hospitals, our households.

The United States has the world's most complex electric grid, and while we have a well-developed system of grid operators to ensure our lights stay on, we're confronting new challenges and adapting to a changing generation mix, new technologies, and consumer preferences. We're also responding to new threats and working to strengthen the cybersecurity of the nation's grid.

The integration into the system of new digital technologies that are essential for keeping up with our nation's energy needs constantly add vulnerabilities. Other vulnerabilities are being added with the increasing dependence on pipeline infrastructure by electric generating units. Combine this with the rapid expansion of cyber capabilities by more of America's adversaries, and safeguarding transmission infrastructure remains particularly urgent.

Many of the federal oversight and regulatory structures in place today, that ensure the system can mitigate and respond to cyber threats can be traced to this Committee's legislative work.

In 2005, we authorized FERC to commission the North American Electric Reliability Corporation (NERC) with the authority to establish and enforce reliability standards and to coordinate activities among industry and the Feds to confront cyber threats.

In 2015, this Committee wrote provisions included in the FAST Act to strengthen DOE's energy sector specific authorities and to facilitate sharing of threat information between private sector asset owners and the federal government. As the federal agency with the leading expertise on our nation's electricity grid and the cybersecurity threats against it, it is imperative that we arm DOE with the tools and authorities to protect our electricity system, from the transmission lines to the generating stations to the pipelines.

Most recently, we developed legislation to elevate DOE's functions overseeing cybersecurity and to improve information sharing, emergency planning and other technical activities in its jurisdiction. That legislative work is continuing,

but fortunately, the Department has used its own authorities to implement enhanced leadership over cybersecurity and to improve interagency coordination.

Against this backdrop, today's hearing provides a great opportunity to update the Subcommittee on what DOE, FERC and NERC are doing to advance cybersecurity practices, protections, and response planning.

I am looking forward to hearing from Assistant Secretary Karen Evans, who heads the DOE Office of Cybersecurity, Energy Security, and Emergency Response, or CESER.

When Ms. Evans testified in September last year, she had been on the job for just a few weeks—though she brought long federal experience to the table as soon as she sat down. So I look forward to discussing DOE's current work, how well it is exercising its coordinating role over the cybersecurity threat, and to learn what challenges she sees going forward, and how she plans to address those challenges.

It will also be helpful to hear today from the regulators of the electric grid: Andy Dodge, who heads FERC's Office of Electric Reliability, and, of course, from Jim Robb, who heads NERC. Both these entities serve at the front lines of regulatory oversight of electric grid infrastructure protection. I'm particularly interested in learning what measures they are working on to address threats, to ensure best practices, and to coordinate response to cyber incidents.

The risks of massive blackouts can be hard to think about. But the cybersecurity realities of today require we face these risks head on, that we be sure our agencies and the appropriate groups have the tools and information they need

to address the risks, and that they are prepared for the consequences of successful attacks.

Thank you, Mr. Chairman for keeping the Subcommittee informed on this important topic.

##